Neurology-Inspired Root Function Protection Scheme for Preventing Intruders from Gaining Access to Critical Functions - Heuristic Footprint Amplification Through Purposeful Kernel Convolution

20 January 2024
Simon Edwards
Research Acceleration Initiative

Introduction

The reliable function of computer systems depends upon certain deep-level elements from the processor and its instruction sets (a potential vulnerability) to an operating environment and its own programming, which introduces its own set of vulnerabilities. From the earliest days of electronic computers, the mitigation of overhead in computational processes has been considered paramount. The entire architecture involved; from hardware to firmware to software; is optimized in such as way that the very deep level functions one wishes most to protect require the *least* processing power to utilize.

While mechanisms exist designed to detect suspicious activity on the basis of electrical usage, heat generation, memory usage, et cetera, an intruder's first step would naturally be to disable or cripple these protections prior to accessing resources substantial enough to trip an alarm. The access to a system kernel would, in and of itself, be unlikely to utilize sufficient resources to trip a heuristic analysis alarm due to the intrinsic efficiency of these deep level functions, *not due to the inadequacy of the heuristic analysis.* Compared to other functions such as graphics rendering and data retrieval (sc. database queries and dumps,) the footprint of unauthorized root level activity is a light one. Therein lies the problem.

Abstract

In human neurology, the brain is able to ensure that essential functions are protected from localized, errant activity in a number of ways. Autonomic functions such as cardiac and respiratory activity are governed by a part of the brain that is isolated from higher brain functions. No combination of higher thought processes (e.g. thinking about apples and elephants at the same time) could cause a person's heart to stop beating. Such trivial minutiae of a human being's everyday mental processes can do nothing to corrupt nor cripple the functions of sensory processing or the autonomic nervous system.

Humans have varying levels of adeptness in contending with distraction with (ibid. previous publication on distractibility) sensory inputs of differing types compromising focus. Higher mental processes are halted and a distraction event occurs when the primary sensory input shifts from one sensory organ to another. The sensation of coldness or wetness of the skin can inhibit the part of the brain responsible for situational awareness and object tracking, for instance (ibid.)

The most fundamental elements of human neurology (sometimes referred to as the reptilian mind) consume the greatest proportion of the brain by volume. Higher brain functions are carried out, principally, in the part of the brain nearest to the meninges (the cortices.) These cognitive zones have been experimentally established to be unrelated to autonomic function, which is dictated the by the brain stem.

In a computer system, the kernel is very much akin to the brain stem and its autonomic functions. It is simplistic, durable and ancient. The designers of operating environments have naturally never considered creating deliberate inefficiencies in the kernel as doing so would hamper system performance.

In applications where data security is paramount, however and keeping in mind, particularly, that high-performance functions can be carried out on mainframes placed physically and logically "behind" secure systems which act as firewalls, the paradigm of highly compact and efficient system kernels is a highly illogical one, from a security standpoint.

Much work has been done to enhance the heuristic analysis of malicious activity, but much as in human neurology, suspicious activity looks, from a heuristic perspective, so similar to ordinary activity that heuristic analysis fails to identify it about 50% of the time. In human neurology, however, thinking about apples and elephants at the same time has never led to widespread systemic dysfunction.

A new security paradigm based upon the enlargement of kernel functions both in terms of the space utilized by the kernel and the diminution of efficiency of kernel functions on an order of magnitude that could be adjusted according to processing capacity (which evolves over time) in order to create operating environments which are structures more like the human brain in the sense that the most essential functions would consume the greatest space, the greatest amount of computational time and also be the most difficult to disrupt or corrupt.

Another metaphor for this type of system would be an automobile in which the low and high gear shifting progression is inverted. In low gear, less force is required to turn a gear at a particular rotational rate. In high gear, a greater amount of force is required to create the same amount of torque. When going up a steep hill, low gear is best because efficiency in generating torque rather than top speed is paramount. 50 years ago, computers needed a lot of "torque" due to the limitations on the computational capacity of CPUs. In terms of heuristic security (whether it is a human being's sanity or a computer's resistance to tampering) the more of the processing capacity and programming is geared toward redundant reinforcement of the most basic functions, the less likely aberrant signals are to substantially disrupt overall function. This may be termed *cognitive inertia.*

In an operating environment with a kernel designed using this distinctly unconventional approach of deliberately introducing inefficiency as well as a

series of non-identical redundancies in kernel function, any utilization of function of such a kernel would generate a highly pronounced heuristic signature. While complex heuristic analysis has logarithmically diminishing returns, *simplistic heuristic analysis with convoluted kernel design* is far more capable of ensuring the detection of unauthorized activity.

Take, for instance, the metaphor of the cat burglar. After entering a building, the cat burglar deliberately treads lightly to avoid the generation of the sound of footfalls or creaks in the floor. A processor-intensive heuristic analysis is akin to placing a series of scales beneath the floorboards in order to detect a cat burglar with the weight of an ant. Convoluted kernel design, by contrast, is a heretofore untried revolutionary approach to computer security which is more akin deliberately installing nothing but creaky floorboards in a room one wishes to secure whilst forcing intruders to carry sandbags into the room with them.

While such a system would have a slow boot time and would suffer from slow performance, the magnified heuristic footprint of intrusion in addition to the deliberately dilatory system performance would enable supporting automated response systems and personnel sufficient time to detect and halt in-process intrusions before a more permanent foothold can be established.

These redundant-yet-unique lines of programming code could be AI-generated as generating functional yet varied patterns of data is an area in which AI excels. From a logical perspective, each sub-section of code would be, in and of itself, incapable of successfully executing code. Only through the use of all sub-sections could functions be executed. This may be facilitated through a redundant series of command encryptions based upon the public key approach. Each sub-section of convoluted kernel would talk to the others through a similar scheme to public-key encryption with the crucial difference being that rather than requiring two keys/algorithms, dozens or hundreds could be required, each managed within the individual sub-domains of kernel. This is akin to communicating with a person at the end of a long series of language translators in which all translators know only the language of the two individuals on either side and do not know any others. The nature of these languages can be reconfigured endlessly in such a scheme. The most important aspect is that the system guarantee that at least a certain number of translation steps occurs between any request and any execution in order to ensure that heuristic "footfalls" are as "loud" as possible. Although "public," each encryption/decryption step would tell its neighbors "how to talk to" the next. As the sub-modules are AI-generated, they could be switched out periodically at little to no cost with the benefit being akin to a top-down redesign of an operating environment by a team of skilled programmers (a process which would ordinarily take years) every few weeks. For security, only the kernel convolution aspect of the operating environment would need to be continually swapped out and this aspect is one which lends itself to automated reprogramming without human intervention.

Conclusion

The advanced state of processor performance and the need for entirely novel approaches to network security recommends this approach as the logical next step in securing critical computer systems. This approach has the advantage of being tunable, meaning that the extent of kernel convolution may be increased as system performance increases.